IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 01-07
www.iosrjournals.org

Advanced Redundancy Management Of Heterogeneous Using The Packet Dropper With Nodes For Multipath routing

Angelin P Edwin
PG Student, Dept of CSE SVS College of Engineering, Coimbatore, Tamilnadu, India.

Abstract: *Developing a secured environment for detectingmalicious nodes in a heterogeneous wireless sensor network(HWSN).Here which is analysing the best redundancylevel using path redundancy and sourceredundancy.Packet droppers with IDS(Intrution detection system)is used for tolerance purpose.To improve this method it uses heterogeneous node for the multipath routing.To deal with packet droppers, a widely adopted counter measure is multipath forwarding.Each packet is forwarding along with multiple redundant paths and some of its path cant be tolerated, this process introducing high extra communications.Here we proposing a probabilistic nested marking(PNM)scheme to identify packet modifiers with a certain probability.In wireless sensor networks(WSN),a critical issue is that security of the data transmission.For the system performance of a WSN,clustering ia an effective and practical way to enhance(CWSN).We proposing two secure and efficient data transmission(SET)protocols for CWSNs,is called SET-IBS (Identity based signature)and SET-IBOOS (Identity-based online/offline signature).*
Keywords: *Heterogeneous wireless sensor network, Multipath routing,Intrusion Detection,Security.*

I. Introduction

The main objective of this project is to develop a secured environment for detecting malicious nodes in a heterogeneous wireless sensor network (HWSN).It is developed by NS2 as the simulation tool.A probability model is used to analyze the best redundancy by using path redundancy and source redundancy.To improve this method here we are using heterogeneous node for multipath routing using packet droppers,which added with IDS(Intrution Detection System) for tolerance purpose.In wireless sensor networks the packet droppers are common attacks to disrupt communication.currently there are of many schemes that have been proposed to mitigate the attacks.But intruders cant be identify effectively and efficiently.we proposing a simple yet effective scheme to addressing the problem.Extensive analysis and simulations using ns2 simulator have been conducted and verified the effectiveness and efficiency of the scheme.

Sensor nodes monitor the environment,detect the events of interest,produce data and collaborate in forwarding the data towards a sink.The sink could be a gateway,basestation,storage node or queringuser.A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection of tasks.When it is deployed in such an environment,it lacks the physical protection and is subject to node compromise.After compromising the one or multiple sensor nodes, a type of various attacks to disrupt in the network communication.Among these attacks,two common ones are dropping packets and modifying packet such as compromised nodes drop or modify the packets that they are supposed to forward.To deal with packet droppers,a widely adopted counter-measure is multipath forwarding in which each packet is forwarded along multiple redundant paths and hence packet droping in some of those paths can be tolerated.This scheme introduces a high extra communication overhead.

Another category of countermeasures is to monitor the bahaviour of forwarding nodes.However,these schemes are subject to high energy cost incurred by the promiscuous operating mode of wireless interface.To deal with packet modifiers most of existing countermeasures are to filter modified messages within a certain number of hops.However without identifying packet droppers and modifiers,these countermeasures cannot fully solve the paket modification problems because the compromised nodes can continue attacking the network without being caught.To identify packet modifiers,Yeet al recently proposed a probabilistic nested marking(PNM) scheme to identify packet modifiers with a certain probability.However,the PNM scheme cannot be used together with the false packet filtering schemes,because the filtering schemes will drop the modified packets which should be used by the PNM scheme as evidenced to infer packet modifiers.This degrades the efficiency of deploying the PNM scheme.

A critical issue in a wireless sensor network(WSNs) is that the security of the data transmission.Clusterinf is an effective and practical way to enhance the system performance of WSNs.Here we showing a secure data transmission for cluster based(CWSNs),where the cluster
are formed dynamically and periodically.We proposing two secure and efficient data transmission(SET)protocols for CWSNs,called SET-IBS and SET-IBOOS,by using the Identity-based digital signature(IBS) scheme and the Identity-Based Online/Offline digital Signature(IBOOS).

In SET-IBS security based on the hardness of the Hellman problem in the pairing domain.SET-IBOOS reduces the computational overhead for protocol security.Here we showing the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks.The calculations and simulations are provided to illustrate the sufficiency of the proposed protocols.the results showing that,the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption .It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data,by applying digital signatures to message packets,which are efficient in communication and applying the key management for security.In the proposed protocols pairing parameters ar distributed and preloaded in all sensor nodes by the base station(BS) initially.

II.Multipath Routing In Wsn

In Wireless sensor networks,which deployed for gathering data from unattended or hostile environment.The existing researches which proposing several application to specify sensor network data for gathering protocols.Most of the proposed algorithm given more attention to these related security issues.Here we explored general security threats in wireless sensor network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them.The networks exposed to various kinds of attacks and conventional defences against to these attacks due to limitations of sensor devices.These attacks are not suitable due to the resource constrained nature of these kinds of networks.Security in WSN is a challenging task due to inheritance limitations of sensors.Here mainly focusing at the secure routing protocols in wireless sensor networks.

Main advantages in communication technology is that allow us to build the networks,where large numbers of low power and it is inexpensive sensor devices, which are integrated in the physical environment and operating together over a wireless media. There are a lot of its application in industry, military and health. Some applications such as intruder detection systems in military, which is the detection of unusual behavior or failures in a manufacturing process or detection of forest fires, and the infrequency of occurrence of specific events has been detected through WSN. The other applications such as monitoring temperature, humidity and lighting in office buildings, data gathering and reporting in the specific periods of time. Some of the applications, the process of gathering and reporting environment data had been asked through the base or sink. The WSN may be used in order to track of specific objects in the environment.Here the above mentioned all applications data has been gathered, and processed via sensor devices in the network. All the collected data based on the transmission is the responsibility of the sensor devices.Hence the development of any routing protocol and more advanced secure routing protocol, the architecture of sensor devices should be determined and also its limitation should be considered .Sensor devices in a WSNs, also may be reffered as sensor node or node, perhaps is the most widely used equipment. It is usually restricted and its name suggests it has the responsibility of sensing environment.It acts as router and transmits data through the wireless medium.The two factors are influenced in routing techniques of wireless sensor networks.First, it deal with hardware and resource constraints.The routing algorithm has to be energy aware, thus it minimize the control information flows and communication the. By the memory capacity the routing table maintanence is limited. Second, through the traffic patterns the nature of sensor network applications are defined,that are different from the traditional ones. It is not necessary to support communication between any pair of nodes the dominant traffic is one-to-many, many-to-one and local communication between neighboursin the sensor networks. Here one-to-many is the base station multicast and many-to-one is the process of data sending to the base station. When the number of nodes are large, the resources are limited.The wireless sensor network usually does not support global addressing, which brings high overhead, it often trade on its data centric character instead and deploys the attribute based addressing that means the base station sends queries for data with specific properties.There are three catagorised routing techniques based on the network structure: flat based, hierarchical based and location based routing.In flat based routed networks, each node plays the same role, due to the large number of nodes the global addressing is not supported, and the data centric approach is used instead. It used a typical algorithm which is Direct Diffusion and Sensor Protocols for Information via Negotiation(SPIN). The cluster based algorithms are using in networks, where the nodes are organized into clusters and route the information via special nodes which denoted as cluster heads. Data aggregation is the main benefit of such type routing algorithms, which saves energy and increases efficiency. The representative of this category is Low Energy Adaptive Clustering Hierarchy (LEACH).

III. Related Work

In this redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user quires in the presence of unreliable and malicious nodes. The main concept of this redundancy management is to exploit the tradeoff between energy consumption with the gain reliability, timeliness, and security to maximize the system useful lifetime.Here which is developing a novel probability

modet to analyze the best redundancy in terms of path redundancy and source redundancy.The lifetime of a HWSN is maximized, when the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval. Applying the analysis results to the design of a dynamic redundancy management algorithm for identifying and applying the best design parameter settings at runtime, when the environment change.

IV. Background And Motivation

Cluster based data transmission in WSNs are to achieve the network scalability and management, that maximizes the lifetime of node and reduce the bandwidth consumption by using local collaboration among sensor nodes. Every cluster has a leader sensor node in a cluster based WSN (CWSN).It regarded as cluster head (CH). A CH that aggregates the data collected by the leaf nodes in its cluster and sends the aggregation to the base station(BS). Heinzelmanet who presented the LEACH (Low Energy Adaptive Clustering Hierarchy) protocol, which willreduce and balance the total energy consumption for CWSNs.To prevent the quick energy consumption of the set of CHs, the LEACH performing randomly rotates at CHs among all sensor nodes in the network,in rounds.The LEACH which can achieves the improvements of network lifetime. Based on this protocol there have been presented such as APTEEN and PEACH.These also using the same concept of the protocol LEACH.The LEACH is a dynamically, randomly and periodically rear range network's cluster and data links. Hence adding the security in LEACH is challenging. The other secure data transmission protocols based on LEACH such as SecLEACH, GS-LEACH and RLEACH. When a node doesnot share a pair wise key with others in its preloaded key ring, in order to mitigate the storage cost of symmetric keys, and the key ring is not sufficient for the node to share pair wise symmetric keys with all of the nodes in a network, it is called an orphan node problem. If it is occurred the cluster cannot participate and has to elect itself as a CH.The Identity based digital signature (IBS), that is based on the difficulty of factoring integers from Identity Based Cryptography (IBC). It is derive an entity public key from its identity information.The IBS is developed as a key management in WSNs for security. To reduce the computation and storage costs of signature processing, the IBOOS scheme is used.Itwas introduced by Even et al.It is effective for the key management in WSNs. The offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed on the time of the communication.

V. System Model

Consider a CWSN consisting of a fixed base station (BS) and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. We assume that the BS is always reliable, which means the BS is a trusted authority (TA). The sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a CWSN, sensor nodes are grouped into clusters, and each cluster has a cluster head (CH) sensor node, which is elected autonomously. Leaf (non-CH) sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs to save energy. The CHs perform data fusion, and transmit the sensed data to the BS directly with comparatively high energy. In addition, we assume that, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained. In CWSNs, data sensing, processing and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate node aggregates data and sends it to the BS is preferred, than the method that each sensor directly sends data to the BS. A sensor node switches into sleep mode for energy saving when it does sense or transmit data, depending on the TDMA (Time Division Multiple Access) control used for data transmission. Here the proposed SET-IBS and SET-IBOOS are both designed for the same scenarios of CWSNs.

For the advanced redundancy management, An Extension for Identifying Packet Modifiers for droppers is implemented. If a compromised node modifies the packets that it is supposed to forward, the node can be detected with the afore-described scheme.This is because, modified packets will be detected by the sink
packets are dropped by the modifier; hence, the packet modifier can be identified as a packet dropper.However, detecting modifiers in this way is not ideal because modified packets cannot be identified earlier by enroute nodes to save energy and bandwidth consumption. To enable enroute detection of modifications, the afore described procedures for packet sending and forwarding can be slightly modified as follows. Whwn a node u has a data item D to report, it can obtain endorsement message authentication codes (MACs) from its neighbours, which are denoted as MAC (D), following existing enroute filtering schemes such as the statistical enroute filtering scheme (SEF) and the interleaved hope by hop authentication scheme. The source node u generates and sends the following packet to its parent node Pu. Our packet dropper/modifier identification scheme is implemented in the ns-2 simulator (version 2.30) to evaluate the effectiveness and efficiency of the proposed scheme. We measure the performance of our scheme from two aspects: the detection rate, defined as the ratio of miscued innocent nodes over all innocent nodes. We run simulations on a 400 £ 400m2 network

with randomly generated network topology. Unless otherwise stated, we set the percentage of bad nodes to 10%, the network size to 100 sensor nodes, the per node packet reporting interval to 3 seconds, and the length of each round to 300 seconds. Also, when a bad node decides to drop packet in a round, ir drops 30% of the packets. In this proposed system, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So we propose two secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS.

VI. Implementation

Pairing for IBS*:* The first functional and efficient ID based encryption based on bilinear pairings on elliptic curves. Specifically, randomly select two large primes's p and q, and let E/Fp indicate an elliptic curve. We denote by G 1aq order subgroup of the multiplicative group in the finite field F * p. The pairing is a mapping e: G1×G1→G2, which is a bilinear map with the following properties.

1.**Bilinear:**∀P,Q,R,S ∈G1,e(P+Q,R+S)=e(P,R)e(P,S)e(Q,R)e(Q,S). In the same way ∀c,d∈ Z * q, e(cP,dQ) = e(P,dQ)c = e(cP,Q)d = e(P,Q)cd, etc.

2.**Non degeneracy:** If P is a generator of G1, then e(P,P) is a generator of G2.

3.**Computability:** There is an efficient algorithm to compute (P,Q)in G2, ∀P, Q ∈ G1.

The security in the IBS scheme is based on the bilinear Diffie Hellman Problem (DHP) in the pairing domain

IBS scheme for CWSNs:This scheme is based on the implementation for CWSNs which consist of the following operations, specifically, setup at the BS, key extraction and signature signing of the data sending nodes, and verification of the data receiving nodes.

1.Setup: The BS generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.

2.Extraction: Given an ID string, a sensor node generates a private key sek ID associated with ID using msk.

3.Signsture signing: Given a message M, time stamp t and a signing key θ, the sending node generates a signature SIG.

4.Verification: Given the ID, M and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject" otherwise.

IBOOS scheme for CWSNs: An IBOOS scheme implemented for CWSNs consist of following four operations, setup at the BS, key extraction and offline signing at the CHs, online signing of the data sending nodes, and verification of the receiving nodes

1.Setup: Same process of the IBS scheme.

2.**Extraction:** Same as that in the IBS scheme.

3.Offline signing: Given public parameters and time stamp t, the CHs, sensor node generates an offline signature SIG offline and transmits it to the leaf nodes in its cluster.

4.Online signing: From the private key sek ID, SIG offline and message M, a sending node generates an online signature SIG online.

5.Verification: Given ID, M and SIG online, the receiving node outputs "accept" if SIG online is valid, and outputs "reject" otherwise.

SET-IBS Protocol: Two novel secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the IBS scheme and the IBOOS scheme, respectively.This is a protocol initialization priorto the network deployment and operates in rounds during communication, which consists of a setup phase and a steady state phase in each round.The protocol initialization which can be describe the key management of the protocol by using the IBS scheme, and the protocol operations afterwards.

(a)Protocol Initialization: Comparing with other LEACH protocols the time in SET-IBS is divided into successive time intervals.Time stamp can be denoted as Ts for BS to node communication and for leaf to CH communication as ti.The key predistribution is an efficient method to improve communication security in WSN.Here we adopt ID ti as user's public key under an IBS scheme,the secure data transmission protocol by using IBS for CWSN (SET-IBS). During the protocol initialization the corresponding private pairing parameters are preloaded in the sensor nodes. When a sensor node wants to authenticate itself to another node, it does not obtain its private key at the beginning of a new round. We using the additively homomorsphism encryption scheme in to encrypt the plaintext of sensed data,so a specific operation performed on the cipher text.By using these techiniques the aggregation of encrypted data at the CHs and the BS, which also guarantees data confidentiality. Based on the protocol initializationthe following operations are performing.Generate an encryption key, Generate the pairing parameters, choosing two cryptographic hash functions, Selecting a random integer, preloading each sensor node with the system parameter.

(b)Keymanagement for security: To adopting the algorithms of IBS from to WSN practically, it simplify the mapping e with one generator P and provide the full algorithm in the signature verification. The proposed SET-

IBS consists of following operations, such as extraction, signing and verification.

(c)Protocol operation: After the initialization of protocol, SET-IBS operates in round during communication.In each round that consists of a setup phase and a steady state phase.We can suppose as the all sensor nodes know the starting and ending time of each round.

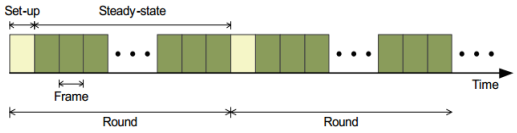

Fig 1.Operation in the proposed secure data transmission.

Set-IBOOS Protocol:The IBOOS scheme based on the DLP in the multiplicative group. Here proposing a secure transmission protocol with IBOOS for CWSNs (SET-IBOOS). During the initialization time the corresponding private pairing parameters are preloaded in the sensor nodes. These also performing the following operations such as extraction, offline signing, online signing and verification.

VII.Results AndDiscusions

The proposed SET-IBS and SET-IBOOS which are essential for prolonging the network lifetime. To evaluate the energy consumption of the computational overhead foe security in communication, we considering three metrics for the performance evaluation : Network lifetime, System energy consumption and the number of alive nodes.

Network lifetime(the time of FND) : We use the most general metric in this paper, the time of FND (first node dies), which indicates the duration that the sensor network is fully functional. Therefore, it maximizing the time of FND in a WSN means to prolong the network lifetime.

The number of alive nodes : The ability of sensing and collection information in a WSN depends on the set of alive nodes (nodes that have not failed). Therefore, we evaluate the functionality of the WSN depending on counting the number of alive nodes in the network.

Total system energy consumption : It refers to the amount of energy consumed in a WSN.we evaluate the variation of energy consumption in secure data transmission protocols.

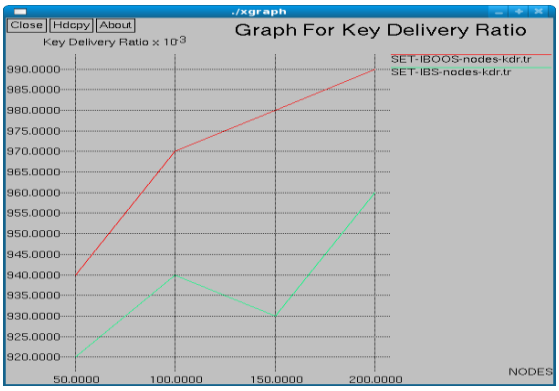

Fig 2. Graph for key delivery ratio

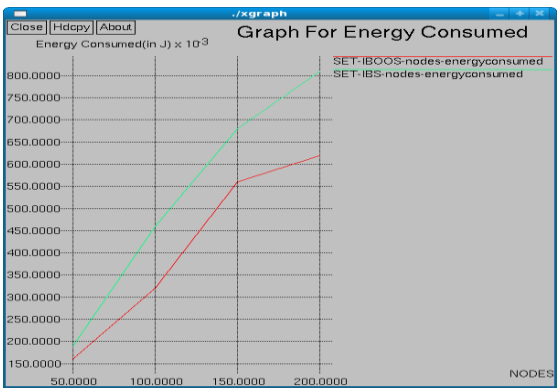

Fig 3. Graph for energy consumed

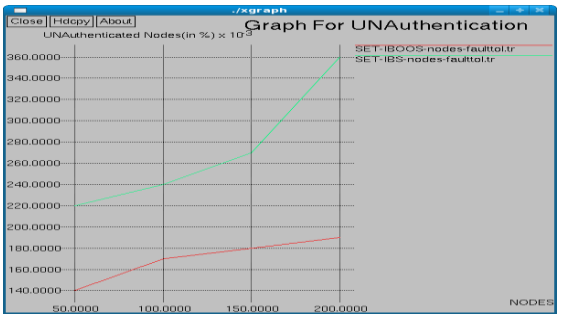

Fig 4. Graph for unauthentication

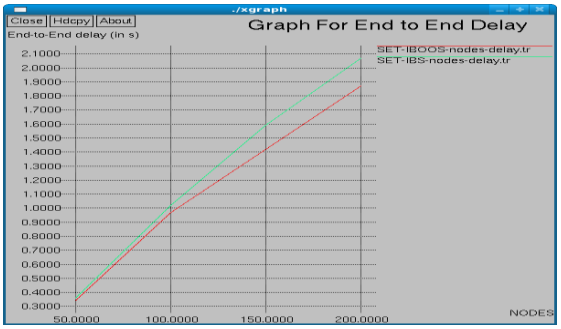

Fig 5. Graph for end to end delay

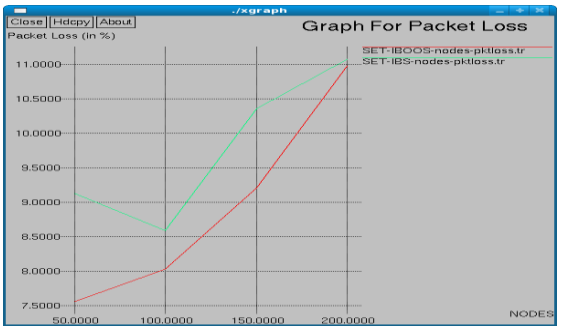

Fig 6. Graph for packet loss

VIII. Conclusion

This paper, which showing the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for data transmission secure has been discussed.Here presented two secure and efficient data transmission protocols respectively for CWSNs,SET-IBS and SET-IBOOS. Providing feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks.Comparison in the calculation and simulation results, that are showing the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. Using the SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs, with respect to the both computation and communication costs.

References

[1] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey,"IEEECommun. Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.

[2] L.Lamport, R. Shostak, and M. Pease, "The byzantine generals prob-lem,"ACM Trans.Programming Languages Syst., vol. 4, no. 3, pp. 382–401, 1982.

[3] Y. Yang, C. Zhong, Y. Sun, and J. Yang, "Network coding based reliable disjoint and braided multipath routing for sensor networks,"J. Netw.Comput. Appl., vol. 33, no. 4, pp. 422–432, 2010.

[4] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing for wireless sensor networks," Computer Commun., vol. 29, no. 2, pp. 216–230, 2006.

[5] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, "Securing geographic routing in wireless sensor networks," in Proc. 2006 Cyber Security Conf. Inf.Assurance.

[6] W. Lou and Y. Kwon, "H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks,"IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1320–1330, 2006.

[7] Y. Lan, L. Lei, and G. Fuxiang, "A multipath secure routing protocol based on malicious node detection," in Proc. 2009 Chinese Control Decision Conf., pp. 4323–4328.

[8] D. Somasundaram and R. Marimuthu, "A multipath reliable routing for detection and isolation of malicious nodes in MANET," inProc. 2008 Int. Conf. Computing, Commun.Netw., pp. 1–8.

[9] H. Su and X. Zhang, "Network lifetime optimization for heterogeneous sensor networks with mixed communication modes," inProc.2007 IEEE Wireless Commun.Netw. Conf., pp. 3158–3163.

[10] I. Slama, B. Jouaber, and D. Zeghlache, "Optimal power management scheme for heterogeneous wireless sensor networks: lifetime maximiza-tion under QoS and energy constraints," in Proc. 2007 Int. Conf. Netw. Services, pp. 69–69.

[11] R. Machado, N. Ansari, G. Wang, and S. Tekinay, "Adaptive density control in heterogeneous wireless sensor networks with and without power management,"IET Commun., vol. 4, no. 7, pp. 758–767, 2010.

[12] E. Stavrou and A. Pitsillides, "A survey on secure multipath routing protocols in WSNs,"Comput.Netw., vol. 54, no. 13, pp. 2215–2238, 2010.

[13] T. Shu, M. Krunz, and S. Liu, "Securedata collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, 2010.

[14] Y. X. Jiang and B. H. Zhao, "A secure routing protocol with mali-cious nodes detecting and diagnosing mechanism for wireless sensor networks," inProc. 2007 IEEE Asia-Pacific Service Comput.Conf.,pp. 49–55.

[15] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," inProc. 2003 IEEE Int. Workshop Sensor Netw. Protocols Appl., pp. 113–127.

[16] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: reliable information forwarding using multiple paths in sensor networks," inProc. 2003 IEEE Conf. Local Computer Netw., pp. 406–415.

[17] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based WSNsUsing ID-Based Digital Signature,"inProc.IEEE GLOBECOM, 2010.

[18] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," inLect. Notes.Comput.Sc. - CRYPTO, 1990.

[19] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures forAODV and DSR Routing Security," inLect.Notes.Comput. Sc. - Inf. Secur.Privacy, 2006.

[20] C.-K. Chu, J. K. Liu, J. Zhou et al., "Practical ID-based encryption for wirelesssensor network,"inProc. ACM ASIACCS, 2010.

[21] C. Karlof and D.Wagner,"Secure routing in wireless sensor networks: attacks andcountermeasures,"Ad Hoc Networks, vol. 1, no. 2-3, 2003.

[22] F. Hess,"Efficient Identity Based Signature Schemes Based on Pairings," inLect.Notes.Comput. Sc. - SAC, 2003.

[23] J. Liu and J. Zhou, "An Efficient Identity-Based Online/Offline Encryption Scheme,"inLect.Notes.Comput. Sc. - Appl. Crypto. Netw.Secur., 2009.

[24] J. J. Rotman, An Introduction to the Theory of Groups. Springer-Verlag; 4thedition, 1994.

[25] K. S. McCurley, "The discrete Logarithm Problem," inProc.Symp. Appl. Math.,Prog. Com. Sc., 1990, vol. 42.

[26] W. Diffie and M. Hellman,"New directions in cryptography," IEEE Trans. Inf.Theory, vol. 22, no. 6, 1976.

[27] D. Boneh, I. Mironov, and V. Shoup, "A Secure Signature Scheme from BilinearMaps," inLect. Notes.Comput. Sc. - CT-RSA, 2003.

[28] P.Barreto,H.Kim,B.Lynn et al.,"Efficient Algorithms for Pairing-BasedCryptosystems," inLect. Notes.Comput.Sc. - CRYPTO, 2002.

[29] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypteddata in wireless sensor networks,"inProc. MobiQuitous, 2005.

[30] H.Lu, J.Li, and G. Wang, "A Novel Energy Efficient Routing Algorithm forHierarchically Clustered Wireless Sensor Networks," inProc. FCST, 2009